Claims

The invention claimed is:

1. A circuit for performing multiplication of two elements from a finite Galois field GF(2^k) wherein said elements are represented by polynomials $a(x)$ and $b(x)$ and multiplication is carried out modulo an irreducible polynomial $p(x)$ of degree k, said circuit comprising:

a first multiplier modulo $p(x)$ for $A_j(x)$ with $(T-1) \geq j \geq 0$ and $b(x)$, where $A_j(x)$ is a polynomial of degree $n-1$ of the form $\Sigma_{i=0}^{n-1} a_{jn+i} x^i$ where a_{jn+i} is the coefficient for the x^{jn+i} term in the polynomial $a(x)$ and wherein $k = nT$;

a summer receiving the output from said multiplier;

a storage means for holding the output from said summer for each of T cycles of operation of said circuit;

a second multiplier modulo $p(x)$ for multiplying the current contents of said storage means by x^n, the output of said second multiplier also being supplied as an input to said summer.

2. The circuit of claim 1 further including means to supply in sequential order T successive representations of said polynomials $A_j(x)$, $(T-1) \geq j \geq 0$, to said first multiplier $A_{T-1}(x)$ being presented first.

3. The circuit of claim 1 wherein said first multiplier multiplies n bit wide representations of $A_j(x)$ with k bit wide representations of $b(x)$.

4. A circuit for performing multiplication of two elements from a finite Galois field GF(2^k) wherein said elements are represented by polynomials $a(x)$ and $b(x)$ and multiplication is carried out modulo an irreducible polynomial $p(x)$ of degree k, said circuit comprising:

a first multiplier modulo $p(x)$ for $A_j(x)$ with $(T-1) \geq j \geq 0$ and $b(x)$, where $A_j(x)$ is a polynomial of degree $n-1$ of the form $\Sigma_{i=0}^{n-1} a_{jn+i} x^i$ where a_{jn+i} is the coefficient for the x^{jn+i} term in the polynomial $a(x)$ and wherein k is not originally equal to nT but where higher order terms in a(x) are added in sufficient number with zero coefficients to insure that k = nT;

a summer receiving the output from said multiplier;

a storage means for holding the output from said summer for each of T cycles of operation of said circuit;

a second multiplier modulo $p(x)$ for multiplying the current contents of said storage means by x^n, the output of said second multiplier also being supplied as an input to said summer.